Docket: M4065.0486/P486 Micron Docket No.: 70-0586

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
APPLICATION FOR U.S. LETTERS PATENT

Title:

METHOD AND APPARATUS FOR WEP KEY MANAGEMENT AND PROPAGATION IN A WIRELESS SYSTEM

Inventor:

Doug Rollins

Dickstein Shapiro Morin &
Oshinsky LLP
2101 L Street, N.W.
Washington, D.C. 20037
(202) 785-9700

TITLE OF THE INVENTION

METHOD AND APPARATUS FOR WEP KEY MANAGEMENT AND PROPAGATION IN A WIRELESS SYSTEM

FIELD OF THE INVENTION

[0001] The present invention relates to generally to network security, and, more particularly to a method and apparatus for encryption key management and propagation in a wireless system.

BACKGROUND OF THE INVENTION

[0002] In a wired LAN, data transmissions are generally regarded as secure. Only those stations physically connected to the wire can receive the LAN traffic. For this reason, significant security precautions are generally not taken to protect the privacy of data transmissions within a LAN.

[0003] A network with wireless stations is not as secure. When data is transmitted to a wireless station, any station within range can eavesdrop on the transmission. The connection of a single wireless link (without any privacy protection) may seriously degrade the security level of the wired LAN.

[0004] Despite the security issues involved in implementing wireless stations, there are many advantages. A company can gain significant advantages by providing wireless connectivity to stations, such as, for example, automatic machinery or equipment that requires rapid deployment within a local area. The stations can be portable, hand-held or mounted on moving vehicles.

[0005] In an effort to preserve network security while using wireless stations, the IEEE has devised Wired Equivalency Privacy ("WEP"). WEP is a cryptographic confidentiality algorithm that can be used to provide data

confidentiality that is subjectively equivalent to the confidentiality of a wired local area network that does not use cryptographic techniques to enhance privacy.

[0006] An example of a wireless network is shown in Fig. 1. Wireless station 100 comprises a wireless network communications device 103, a microprocessor 101 and a data storage area 102. Wireless communications device 103 can be a wireless network interface card. Data storage area 102 stores the operating system and the support application for wireless station 100. An encryption key is stored within the support application.

[0007] Wired station 110 comprises a network communications device 113, a microprocessor 111 and a data storage area 112. Data storage area 112 stores the operating system and management application for wired station 110. Access point 120 is physically connected to wired station 110. Access point 120 is a bridge between the Ethernet network and the wireless network. These devices are well known in the art.

[0008] The process for updating encryption keys in a wireless network, such as that shown in Fig. 1, implementing WEP is shown in Fig. 2. The process begins when the network administrator selects a new encryption key at segment 200. IEEE 802.11x standard suggests a 40-bit or 128-bit encryption key, however, any convenient length may be used. The network administrator then propagates the new encryption key to access point 120. This can be accomplished one of two ways. If the vendor supplies a management application that supports automatic propagation to access points, then that may be used. If the vendor supplied management application does not provide the ability to automatically propagate new encryption keys to access points, the network administrator must manually enter the new encryption key at each access point. This entails writing the encryption key down and then manually entering it into the access point management application.

[0009] Once the encryption key at access point 120 is updated, no wireless network traffic can be decrypted by wireless station 100 until the encryption key at wireless station 100 is updated to match the updated encryption key at access point 120. In order to update the encryption key at wireless station 100 at segment 210, the network administrator must manually enter the new encryption key at wireless station 100. The encryption keys are stored in the software associated with wireless network communications device 103. As a result, the network administrator must physically access wireless station 100, start the operating system, open wireless communications device 103's support application and manually enter the WEP key at segment 210. This process must then be repeated for each wireless station.

[0010] Due to the cumbersome nature of manually changing the encryption keys at every wireless station, network administrators are reluctant to update encryption keys on a regular basis. When they do update the encryption key, it is a time-consuming task.

[0011] A quick, easy and secure method and apparatus for updating encryption keys in a wireless network is desirable.

SUMMARY OF THE INVENTION

[0012] The present invention mitigates the problems associated with the prior art and provides a unique method and apparatus for encryption key management and propagation in a wireless system.

[0013] In accordance with an exemplary embodiment of the present invention, an encryption key is stored in a removable wireless network communications device in each wireless station. When an encryption key is to be updated, the wireless network communications device card is removed from the wireless station and inserted into a card tray connected to a wired portion of the

network. A management station randomly generates a new encryption key and propagates it to all access points and to one or more card trays. The card trays may be conventional personal computer card trays, e.g. PCMCIA or other PC card trays. Once the encryption key is updated at each access point and the one or more PC card trays and the encryption key in each of the wireless network communications devices is updated. The wireless network communications devices having updated encryption keys may then be removed from the card trays and reinserted into the wireless stations.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The above and other features and advantages of the invention will be more readily understood from the following detailed description of the invention which is provided in connection with the accompanying drawings.

[0015] Fig. 1 is a block diagram of a wireless network;

[0016] Fig. 2 is a flowchart of the process of updating the encryption keys in a wireless network in the prior art;

[0017] Fig. 3 is a flowchart of an exemplary embodiment of the present invention; and

[0018] Fig. 4 is a block diagram of a wireless network implementing an exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0019] In the following detailed description, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to make and use the invention, and it is to be understood that structural

changes may be made and equivalent structures substituted for those shown without departing from the spirit and scope of the present invention.

[0020] Fig. 3 shows an exemplary embodiment of the present invention implemented on the network shown in Fig. 4. Fig. 4 is identical to Fig. 1 except for the addition of a card tray 400 ("PC card tray"). The card tray may receive any type of conventional computer card, but for purposes of simplifying discussion, it will be assumed that the network communications devices are provided on a PCMCIA card and that the card tray 400 receives such cards. PCMCIA (Personal Computer Memory Card International Association) established standards for memory and I/O devices for personal computers. PC card tray 400 has a plurality of slots each of which can receive an inserted wireless network communications device 103 that meets the PCMCIA standards. When wireless network communications device 103 is inserted into a slot of PC card tray 400, and the PC card tray 400 receives a new encryption key, PC card tray 400 accesses the encryption key stored in wireless communications device 103, erases the old encryption key and stores the updated encryption key. Additionally, if a PC card tray 400 has already received a new encryption key when wireless communications device 103 is inserted, PC card tray 400 can then access the encryption key stored in wireless communications device 103, erase the old encryption key and store the updated encryption key.

[0021] Referring to Fig. 3, in an exemplary embodiment of the present invention, management station 110 checks the encryption key generation and propagation schedule at segment 300. If it is not a scheduled time to propagate a new encryption key, as determined at processing segment 305, management station 110 returns to segment 300. If management station 110 determines that it is time to propagate a new key according to the encryption key generation and

propagation schedule at processing segment 305, management station 110 generates a new encryption key at segment 310.

[0022] The encryption key generation and propagation schedule can be determined by the network administrator. Encryption key updates can be set to take place on specific days at specific times, at specified intervals (e.g. every Monday), randomly or whenever a network administrator wants to change the encryption key. Once the network administrator determines how often to update the encryption keys, the network administrator can set the system to either automatically propagate the new encryption keys on schedule or to alert the network administrator to propagate the new encryption key.

[0023] Scheduled encryption key updates has several advantages. First, network security will not be compromised by extended periods of time using the same encryption key. Second, since management station 110 is generating the encryption key, rather than the network administrator, the encryption key is randomly generated. A randomly generated encryption key provides for greater security than a manually chosen one.

[0024] Security can be further enhanced if the same encryption key is not frequently reused. Thus, the system may also be set to prevent re-use of encryption keys. Accordingly, once a new encryption key is generated at segment 310, management station 110 verifies that the randomly generated encryption key is not identical to any of the 4 encryption keys that were previously used at processing segment 315. The number of previous encryption keys that each new encryption key is checked against can be set by the network administrator at management station 110. If the encryption key randomly generated at segment 310 matches one of the previous 4 encryption keys used, as determined at processing segment 315, that encryption key is discarded and

management station 110 returns to segment 310 to randomly generate a new encryption key.

[0025] After management station 110 randomly generates an encryption key that is not identical to any of the previous 4 encryption keys, the new encryption key is propagated to all WEP-enabled devices at segment 320. Access points 120 and PC card trays 400 all store the new encryption key.

[0026] In a preferred embodiment of the present invention, there are two types of encryption key capable devices. First, there are the access points. Access points are bridges between the Ethernet network and the wireless network. These devices are well known in the art. Second, there are PC card trays. The PC card trays are connected to the wired Ethernet and can have multiple PC cards inserted simultaneously for encryption key updating. A crucial improvement of the present invention is that the encryption key is stored in wireless communications device 103 rather than in data storage area 102. As a result, wireless communications device 103 can be removed from wireless station 100 and inserted into PC card tray 400 to be updated. Once wireless communications device 103 is inserted into PC card tray 400 and the PC card tray 400 receives a new encryption key, the PC card tray 400 enables access to the encryption key stored in wireless communications device 103, the new updated encryption key is stored in wireless communications device 103. PC card trays can be connected to the wired Ethernet at any convenient location.

[0027] By allowing wireless communications device 103 to be updated by placing it in PC card tray 400, greater network security and reliability is achieved. First, since the encryption key is not written down and entered manually, there is no chance of the network administrator making an error while typing in the new encryption key. Second, since not even the network administrator knows what the encryption key is, the only way to obtain the

encryption key is by gaining physical access to the network. Third, the network administrator does not have to physically access each wireless station 100. A technician, or even the user, can remove network communications device 103 from wireless station 100 and insert it into PC card tray 400. There can be many PC card trays connected to the wired network and placed at convenient locations so that the inconvenience is minimized.

[0028] If the device being updated is an access point, as determined at processing segment 325, then the encryption key is updated at segment 330. If the update is successful, as determined at processing segment 335, success is reported to management station 110 at segment 337. If the update is not successful, as determined at processing segment 335, failure is reported to management station 110 at segment 336. Management station 110 can then alert the network administrator of the failure so that the problem can be corrected. If the device is not an access point, as determined at processing segment 325 and if the device is not a PC card tray 400, as determined a processing segment 340, e.g. it is a wired station of the wired network, the process ends.

[0029] If the device is a PC card tray 400, as determined at processing segment 340, the encryption key of the wireless communications device 103 in the first slot of PC card tray 400 is updated at segment 345. The encryption key stored in wireless communications device 103 can also be updated after the new encryption key has been propagated to the network by inserting it into PC card tray 400. If the encryption keys in all network communications devices 103 in PC card tray 400 have not been updated, as determined at processing segment 350, the network communications device 103 in the next slot of PC card tray 400 is updated at segment 360. If the encryption keys in all network communications devices 103 in PC card tray 400 have been updated, as

determined at processing segment 350, success is reported to management station 110 at segment 355.

[0030] While the invention has been described with reference to exemplary embodiments various additions, deletions, substitutions, or other modifications may be made without departing from the spirit or scope of the invention. Accordingly, the invention is not to be considered as limited by the foregoing description, but is only limited by the scope of the appended claims.